HKUST – Department of Computer Science and Engineering
COMP170: Discrete Math Tools for CS – Spring 2011

#	LS

Midterm Examination 2

Solution Key

Name: _____	Student ID: _____
Email: _____	Lecture and Tutorial: _____

Instructions

- This is a closed book exam. It consists of 14 pages and 7 questions.
- Please write your name, student ID, email, lecture section and tutorial on this page.
- Please sign the honor code statement on page 2.
- Answer all the questions within the space provided on the examination paper. You may use the back of the pages for your rough work. The last three pages are scrap paper and may also be used for rough work. Each question is on a separate page. This is for clarity and is not meant to imply that each question requires a full page answer. Many can be answered using only a few lines.
- **Unless otherwise specified you *must* always explain how you derived your answer. A number without an explanation will be considered an incorrect answer.**

Questions	1	2	3	4	5	6	7	Total
Points	16	17	18	18	9	10	12	
Score								

As part of HKUST's introduction of an honor code, the HKUST Senate has recommended that all students be asked to sign a brief declaration printed on examination answer books that their answers are their own work, and that they are aware of the regulations relating to academic integrity. Following this, please read and sign the declaration below.

I declare that the answers submitted for this examination are my own work.

I understand that sanctions will be imposed, if I am found to have violated the University regulations governing academic integrity.

Student's Name: _____

Student's Signature: _____

Problem 1 [16 pts]

Evaluate the following expressions and show your calculations.You must not use repeated squaring.

(a) $3^{1081} \bmod 7$.

(b) $180^{60} \bmod 61$.

(c) $183^{60} \bmod 61$.

(d) $10^{13} \bmod 26$.

Solution:

(a)

$$\begin{aligned} & 3^{1081} \bmod 7 \\ = \; & 3^{(6\cdot 180+1)} \bmod 7 \\ = \; & (3 \cdot (3^6)^{180}) \bmod 7 \\ = \; & ((3 \bmod 7)((3^6) \bmod 7)^{180}) \bmod 7 \\ = \; & 3 \bmod 7 \qquad \text{(by the fermat's little theorem)} \\ = \; & 3 \end{aligned}$$

(b) $180^{60} \bmod 61 = (180 \bmod 61)^{60} \bmod 61 = 58^{60} \bmod 61 = 1$ by the fermat's little theorem.

(c) $183^{60} \bmod 61 = 0$ since 183 is multiple of 61.

(d) By Euclid's division theorem, we have

$$\begin{aligned} r &= 10^{13} \bmod 26 \\ &= 10^{13} - 26q \\ &= 2(5 \cdot 10^{12} - 13q) \end{aligned}$$

where $0 \leq r < 26$. This implies $0 \leq \frac{r}{2} < 13$ and thus

$$\frac{r}{2} = 5 \cdot 10^{12} mod 13 = 5$$

.

Therefore,

$$r = 10$$

Problem 2 [17 pts]

Consider the following two sets of modular equations:

(a)

$$\begin{aligned} x \bmod 20 &= 1 \\ x \bmod 21 &= 3 \end{aligned}$$

(b)

$$\begin{aligned} x \bmod 15 &= 1 \\ x \bmod 21 &= 3 \end{aligned}$$

For each of the two sets of equations answer the following question:

> Does there exist a solution for $x \in Z_{mn}$, where m and n are the divisors of the two modular equations?

Note: in (a), $(m, n) = (20, 21)$; in (b), $(m, n) = (15, 21)$.

For each set, explain why your answer is correct. Furthermore, if your answer is that there is a solution, give a solution.

Solution:

(a) Since $gcd(21, 20) = 1$, the Chinese Remainder Theorem tells us that there is a unique solution to this problem.
Running the Extended GCD algorithm gives $1 = 21 \cdot 1 + 20 \cdot (-1)$.
Thus, the multiplicative inverse of 20 in Z_{21} is $-1 \bmod 21 = 20$ and the multiplicative inverse of 21 in Z_{20} is 1. Set $y = 1 \cdot 21 \cdot 1 + 3 \cdot 20 \cdot 20$ and then set $x = y \bmod 420 = 381$ to be the answer.

(b) There is no solution.
By contradiction, suppose that there was some solution x.
Since $x \bmod 21 = 3$ implies $x = 21q + 3 = 3(7q + 1)$ for some integer q. Thus, 3 divides x, i.e. $x = 3k$ for some k.
On the other hand, since $x \bmod 15 = 1$, we have $x = 15q' + 1$ for some q'. This implies $1 = x - 15q' = 3(k - 5q')$, so 3 divides 1. This is false, and thus there is no solution to the problem.
Note that saying that $gcd(21, 15) = 3 \neq 1$ is not a sufficient answer to this question, since it does not guarantee the non-existence of a solution.

Problem 3 [18 pts]

Suppose when applying RSA that, $p = 7$, $q = 11$, and $e = 13$.
(a) What are the values of n and d?
(b) Show how to encrypt the message $M = 50$, and then how to decrypt the resulting message. Use *repeated squaring* for THE encryption and decryption.

Solution:

(a) $n = pq = 77$.
Let $T = (p-1)(q-1) = 60$. d should be the value s.t. $ed \bmod T = 1$, i.e. $13 \cdot d \bmod 60 = 1$.
Running the extended GCD algorithm gives $d = -23 \bmod 60 = 37$.

(b) Let C be the encrypted message, we have $C = 50^e \bmod n = 50^{13} \bmod 77 = 50^{(2^3+2^2+2^0)} \bmod 77$. By repeated squaring, we have $I_0 = 50$, $I_1 = 36$, $I_2 = 64$, $I_3 = 15$. Thus, $C = (15 \cdot 64 \cdot 50) \bmod 77 = 29$.

Let Z be the decrypted message from C, we have $Z = 29^d \bmod n = 29^{37} \bmod 77 = 29^{(2^5+2^2+2^0)} \bmod 77$. By repeated squaring, we have $I_0 = 29$, $I_1 = 71$, $I_2 = 36$, $I_3 = 64$, $I_4 = 15$, $I_5 = 71$. Thus, $Z = (71 \cdot 36 \cdot 29) \bmod 77 = 50$.

Problem 4 [18 pts] For each of the following pairs of logical statements, either prove that the two statements are logically equivalent, or give a counterexample. In your proof, you may use either truth table or logic laws. A counterexample should consist of a truth setting of the variables and the truth values of the statements under the setting.

(a) $p \Rightarrow q$ and $q \Rightarrow p$

(b) $p \Rightarrow q$ and $\neg q \Rightarrow \neg p$

(c) $(p \Rightarrow p) \Rightarrow q$ and $p \Rightarrow q$

(d) $(p \Rightarrow p) \Rightarrow q$ and q

(e) $q \Rightarrow (p \wedge \neg p)$and $\neg q$

(f) $q \Rightarrow (p \wedge \neg p)$ and $\neg p$

Solution:

(a) False. Set $p = T, q = F$. $p \Rightarrow q = F$, but $q \Rightarrow p = T$.

(b) True. $p \Rightarrow q \equiv \neg p \vee q \equiv (\neg\neg q) \vee (\neg p) \equiv \neg q \Rightarrow \neg p$. Or truth table

p	q	$p \Rightarrow q$	$\neg q$	$\neg p$	$\neg q \Rightarrow \neg p$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

(c) False. Set $p = F, q = F$. $(p \Rightarrow p) \Rightarrow q = F \neq p \Rightarrow q = T$.

(d) True. $(p \Rightarrow p) \Rightarrow q \equiv T \Rightarrow q \equiv q$. Or use true table

p	q	$p \Rightarrow p$	$(p \Rightarrow p) \Rightarrow q$	q
T	T	T	T	T
T	F	T	F	F
F	T	T	T	T
F	F	T	F	F

(e) True. $q \Rightarrow (p \wedge \neg p) \equiv q \Rightarrow F \equiv \neg q$. Or use true table

p	q	$p \wedge \neg p$	$q \Rightarrow (p \wedge \neg p)$	$\neq q$
T	T	F	F	F
T	F	F	F	F
F	T	F	T	T
F	F	F	T	T

(f) False. Set $p = T, q = F$. $q \Rightarrow (p \wedge \neg p) = T \neq \neg p = F$.

Problem 5: [9 pts]

For each of the logic statements on the left, circle a statement on the right that is equivalent to it. There is no need to justify your answer.

(i). $\exists x(P(x) \vee Q(x))$	(a). $\forall x(P(x) \wedge Q(x))$ (b). $\neg(\forall x \neg P(x)) \vee \neg(\forall x \neg Q(x))$ (c). $\neg(\forall x \neg P(x)) \wedge \neg(\forall x \neg Q(x))$ (d). $\neg(\forall x \neg P(x)) \vee (\forall x \neg Q(x))$
(ii). $\exists x P(x) \Rightarrow \forall y Q(y)$	(a). $\exists x \neg P(x) \vee \forall y Q(y)$ (b). $\exists x \neg P(x) \wedge \forall y Q(y)$ (c). $\exists x \neg P(x) \Rightarrow \forall y Q(y)$ (d). $\forall x \neg P(x) \vee \forall y Q(y)$
(iii). $\neg\forall x \exists y(A(y) \wedge B(x,y))$	(a). $\forall x \forall y(A(y) \Rightarrow \neg B(x,y))$ (b). $\exists x \forall y(A(y) \Rightarrow \neg B(x,y))$ (c). $\forall x \forall y(A(y) \Rightarrow B(x,y))$ (d). $\forall x \exists y(A(y) \Rightarrow B(x,y))$

Solution:

(i) (b)

(ii) (d)

(iii) (b)

Problem 6: [10 pts]

Let a and n be two positive integers. Prove the following statement by contraposition:

> If there exist integers x and y such that
> $ax + ny = 1$, then a and n are relatively prime.

Solution:

By contraposition, to prove the given statement, it is equivalent for us to prove: If a and n are not relatively prime, then there is no integer pair (x, y) such that $ax + ny = 1$.

Suppose a and n are not relatively prime. Let d be a common factor of them that is larger than 1, and $a = dp$ and $n = dq$ where p and q are integers. Therefore $ax + ny = dpx + dqy = d(px + qy)$. No integer pair (x, y) can make $ax + ny$ equal to 1 because $d > 1$ and $(px + qy)$ is an integer.

Problem 7: [12 pts]

Let a and b be two integers such that $0 \leq a < b$. Prove by induction that for any integer $n \geq 1$, $b^n - a^n$ is divisible by $b - a$.

Solution:

Let $T(n) = b^n - a^n$, $P(n)$ denote: $(b-a)|T(n)$.

Base Case $n = 1$, $T(1) = b - a$, $(b-a)|(b-a)$, so $P(n)$ is true when $n = 1$.

Induction Case Assume that $P(n)$ is true when $n = k - 1$, that is, $(b-a)|(b^{k-1} - a^{k-1})$.

$$\begin{aligned} T(k) &= b^k - a^k \\ &= b^{k-1} \cdot b - b^{k-1} \cdot a + b^{k-1} \cdot a - a^{k-1} \cdot a \\ &= b^{k-1}(b-a) + (b^{k-1} - a^{k-1})a \\ &= b^{k-1}(b-a) + T(k-1)a \end{aligned}$$

$\because (b-a)|T(k-1)$, $\therefore (b-a)|T(k-1)a$.
$\therefore (b-a)|T(k)$.

Therefore, P(n) holds for every integer $n \geq 1$.